ORDERLY ALGORITHM TO ENUMERATE CENTRAL GROUPOIDS

TIME'S UP WORKING PAPERS - 2003-CG-2

TIM BOYKETT TIM@TIMESUP.ORG TIME'S UP RESEARCH DEPARTMENT AND DEPARTMENT OF MATHEMATICS, KEPLER UNIVERSITY, LINZ, AUSTRIA

Abstract. Using an orderly algorithm to determine the complete collection of all graphs with a unique path property seems like a good idea. It works better by a detour.

A graph has the unique path property UPP_n if there is a unique path of length n between any ordered pair of nodes.

This paper reiterates Royle and MacKay's technique for constructing orderly algorithms. We wish to use this technique to enumerate all UPP_2 graphs of small orders 3^2 and 4^2. We attempt to use the direct graph formalism and find that the algorithm is inefficient.

We introduce a generalised problem and derive algebraic and combinatoric structures with appropriate structure. We are able to then design an orderly algorithm to determine all UPP_2 graphs of order 3^2, which runs fast enough. We hope to be ble to determine the UPP_2 graphs of order 4^2.

1. Introduction

Orderly algorithms are a concept for enumerating combinatoric objects: trees, graphs, flocks and many other objects have been approached in this way. The essential hope is to efficiently enumerate the objects without generating isomorphs: by cutting down the production, there is no need to filter the isomorphs out afterwards.

Central groupoids were introduced by Evans in the late 1960s. Knuth later showed that central groupoids are equivalent to a matrix problem proposed by Hoffman: which 0-1 matrices A exist such that $A^2 = J$ where J is the matrix consisting of all 1s. This is equivalent to the problem of determining those directed graphs with exactly one path of length two between any pair of nodes. Shader has shown that matrices of all possible ranks exist. A series of papers by various researchers has investigated generalisations of this problem and special solutions, but until recently exhaustive lists of examples of nontrivial order have not been published. Recently a report listing all examples of order 9 has appeared. In the following we will confirm these results, using techniques that should be extendable to further listings.

Date: October 2003.

This report is structured as follows. We introduce the orderly algorithm as formulated by Royle, based upon the McKay formulation. This technique is particularly suitable to structures that can be formulated in some way as graphs, which will be our case. We will then look at the central groupoids; some general theory and some existence results. Although there would seem to be a good connection between the graph model of central groupods and the orderly algorithm model of Royle, this turns out to be inappropriate. We introduce a generalisation of central groupoids and a derived combinatorial structure. It turns out that this can be used in an orderly algorithm to efficiently enumerate examples. We then use the theory connecting central groupoids to these generalisations in order to filter out the desired examples.

The implementation in GAP [GAP02] using the GRAPE [Soi93] package is discussed. GAP is a programming environment for group theory and other algebraic programming. GRAPE is used for graph manipulation and to access the `nauty` [McK90] package for graph automorphism.

We restrict ourselves to finite examples throughout.

2. Orderly Algorithms

A standard way to generate examples of combinatorial structures is to generate examples in a way that can be proven to be exhaustive, and then remove isomorphs from the list. This can be simple and effective, but if we generate too many examples, then the effort required to filter out the isomorphs can be overwhelming, owing to the quadratic growth of the number of comparisms, a process that is often complex.

An alternative approach is to ensure that the branching generation process does not generate isomorphic examples, thus removing the filtering step of the algorithm described above. With careful bookkeeping, this can be done. Such generation processes have been called "orderly" in [Rea78]. McKay has developed a general structure for such algorithms [McK98] and Royle has developed a simplified algorithm [Roy98], upon which we base ours.

Let V be some set, G a group acting upon V. We write v^g for the action of $g \in G$ on $v \in V$ and extend naturally to actions on sets. We want to find all subsets $X \subset V$ such that $P(X)$ is true for some hereditary property P, but we want only one example from each isomorphism class, with isomorphism defined by G.

We require a function Θ such that

$$\Theta : 2^V \to 2^V \tag{2.1}$$

$$\Theta(X) \text{ is an orbit of } G_X \text{ on } X \tag{2.2}$$

$$\Theta(X^g) = \Theta(X)^g \forall g \in G \tag{2.3}$$

where G_X is the stabiliser of X, $G_X = \{g \in G | X^g = X\}$.

Let T_k be the set of sets of size k such that $P(X)$ is true for all $X \in T_k$, and T_k contains no isomorphs. The following algorithm generates a set T_{k+1} from T_k.

```
T_{k+1} := ∅
for X in T_k do
  for x representative in each orbit of G_X upon V - X do
    if P(X + x) and x ∈ Θ(X + x) then
      add X + x to T_{k+1}
    endif
  enddo
enddo
```

Theorem 2.1 (Royle[Roy98], McKay [McK98])**.** *Let T_k contains exactly one representative from each G–orbit on k–sets of V that have property P. Then the set T_{k+1} generated by the algorithm above contains exactly one representative from each G–orbit on $k+1$–sets of V that have property P.*

Starting with $T_0 = \{\emptyset\}$ we obtain an orderly algorithm for constructing one representative of each subset of V with property P.

Royle's technique for orderly algorithmic generation has been applied to a number of problems, mostly in the area of flocks and related structures in finite geometries.

One main problem is to define the function Θ.

One property of the `nauty` package is that it constructs a *canonical labelling* of a graph. A canonical labelling uniquely identifies each node of a graph up to automorphisms.

Definition 2.2. *A* canonical mapping α *takes a graph* $\Gamma = (N, E)$ *and maps*

$$\alpha : \mathcal{G} \rightarrow (\mathcal{N} \rightarrow \mathbf{N}) \tag{2.4}$$

$$\alpha : \Gamma = (N, E) \mapsto \alpha_\Gamma : N \rightarrow \{1, \ldots |N|\} \tag{2.5}$$

s.t. for any bijection $\phi : N \rightarrow M$, $\forall n \in n, m \in M$,

$$\alpha_{\Gamma^\phi}(m) = \alpha_\Gamma(n) \Rightarrow \exists \psi \in Aut(\Gamma), \phi(n^\psi) = m \tag{2.6}$$

One such function is available in GAP using the GRAPE package which forms an interface to the nauty package. With this canonical mapping we can work wonders; this is in some sense the magic bullet for Royle's algorithm.

Definition 2.3. *Let $f : 2^V \rightarrow \mathcal{G}$ be a mapping from subsets of V to the class of digraphs. Let $X \subseteq V$, $f(X) = (N, E)$ and $f_X : X \rightarrow N$ such that $\forall g \in G$ there exists an isomorphism $\phi_g : f(X) \rightarrow f(X^g)$ such that $f_{X^g} \circ g = \phi_g \circ f_X$ and for all $\phi \in Aut(f(X))$ there exists $g \in G_X$ such that $\phi = \phi_g$. We call such a pair of mappings a* canonical embedding.

This definition means that we can embed our sets X into some class of graphs such that the automorphisms of X, G_X and the automorphisms of the class of graphs coincide properly. We may need to make a complex embedding in order to prohibit extra automorphisms from arising.

Proposition 2.4. *Let f define a canonical embedding, α a canonical mapping. Define $\Theta(X) = x^{G_X}$ with $\alpha_{f(X)}(f_X(x))$ minimal in $\alpha_{f(X)}(f_X(X))$. Then Θ satisfies the requirements for an orderly algorithm.*

Proof. The first two properties required of Θ are apparent.

Let $g \in G$ be arbitrary but fixed. Define $x_1, x_2 \in X$ such that $\alpha_{f(X)}(x_1)$ is minimal and $\alpha_{f(X^g)}(x_2^g)$ is minimal. Since they are both minimal in $1 \dots |X|$ they are equal, so by the canonical mapping property there exists $\psi \in Aut(f(X))$ such that

$$\phi_g \psi(f_X(x_1)) = f_{X^g}(x_2^g)$$

Since

$$\phi_g^{-1} f_{X^g}(x_2^g) = \phi_{g^{-1}} f_{X^g}(x_2^g) = f_X g^{-1}(x_2^g) = f_X(x_2)$$

Using the property of a canonical embedding, and the fact that the automorphism ψ can be represented as ϕ_h for some $h \in G_X$, we obtain

$$f_X(x_2) = \phi_h f_X(x_1) = f_X(x_1^h) \Rightarrow x_2 = x_1^h.$$

We know $\Theta(X) = x_1^{G_X}$ and $G_{X^g} = g^{-1} G_X g$. Then

$$\begin{align} \Theta(X^g) &= (x_2^g)^{G_{X^g}} = x_2^{g g^{-1} G_X g} \tag{2.7} \\ &= (x_2^{G_X})^g = (x_1^{G_X})^g = \Theta(X)^g \tag{2.8} \end{align}$$

and we are done. □

Definition 2.5. *A mapping $v : 2^V \times V \to O$, O an ordered set, is a* combinatorial value *if $v(X, x) = v(X^g, x^g)\ \forall g \in G$.*

We usually take O to be the integers, or the set of n–tuples ordered lexicographically.

Corollary 2.6. *Let $v_i, i = 1, \dots, n$ be combinatorial values on V. With terms as in the previous Proposition, requiring $(v_1(X, x), \dots, v_n(X, x), \alpha_{f(X)}(f_X(x))$ to be minimal in $\{(v_1(X, x), \dots, v_n(X, x), \alpha_{f(X)}(f_X(x)) : x \in X\}$ gives a Θ that satisfies the requirements of an orderly algorithm.*

Proof. If x is such that $v_i(X, x)$ is uniquely minimal, then we have determined a node uniquely. Thus $\Theta(X) = \{x\}$, so $\Theta(X^g) = \{x^g\} = \Theta(X)^g$ and we are done.

Otherwise we select our minimal x as in Proposition 2.4 from a union of orbits of G_X on X. This union of orbits is covariant across isomorphisms, so we can use the same argument as in the proof of Proposition 2.4. □

We can compute this $n+1$–tuple stepwise; if $v_i(X,x)$ is not minimal then we know that x is not in the orbit $\Theta(X)$. If $v_i(X,x)$ is uniquely minimal for all $x \in X$, then it is in $\Theta(X)$ and we can stop and accept the extension (because $x \in \Theta(X)$), without having to compute the following $v_j(X,x)$ or the canonical labelling. Otherwise we carry on to the next element of the tuple. Only in some cases do we need to compute the canonical labelling.

In fact we could compute the orbits of G_X on the elements x with $(v_1(X,x),\ldots,v_n(X,x))$ minimal. If there is only one orbit, then $\Theta(X)$ must be this orbit. This removes further determinations of the canonical mapping. However, in GRAPE we obtain the automorphism group of the graph and the canonical mapping at the same time, so we do not save any computation.

3. Central Groupoids

Evans [Eva67] investigates the various products that can be defined on the set $S = A \times A$ for some set A. A well–known example of such a construction is the rectangular semigroup [McL54], where one takes a pair of sets A, B, forms the product $S = A \times B$ and the product $(a,b) * (c,d) = (a,d)$. This is an idempotent semigroup satisfying the axiom $a * b * a = a$ for all $a, b \in S$, and every semigroup satisfying this equation is of this form.

Evans looked at all the possible products on $S = A \times A$, and found that other than the rectangular semigroups, the only other interesting examples were defined by

$$(a,b) \bullet (c,d) = (b,c). \tag{3.1}$$

This operation satisfies the identity $(a \bullet b) \bullet (b \bullet c) = b$.

Definition 3.1. *A* Central Groupoid *is a* (2)*-algebra* $(S,\bullet)$ *satisfying the axiom:*

$$(a \bullet b) \bullet (b \bullet c) = b \tag{3.2}$$

The examples used by Evans are referred to as the *natural* central groupoids. All natural central groupoids have, by construction, order equal to a square. In a natural central groupoid, we see that $(a,b) \bullet (a,b) = (a,b)$ iff $a = b$, thus we have $|A|$ idempotents in a natural central groupoid of order $|A|^2$. These are general results for central groupoids.

Theorem 3.2 (Evans, Knuth)**.** *If* $(S,\circ)$ *is a finite central groupoid, then* $|S| = n^2$ *for some integer* n*. For every positive integer* n *there exists a central groupoid of order* n^2*. In any finite central groupoid of order* n^2*, the number of idempotents is* n*.*

Note that the first result appears as Corollary 5.14, the second follows from the example above. The third result is very difficult to show in an algebraic setting, we need to move over to a matrix theoretic setting in order to prove it [Knu70].

In [Knu70], Knuth investigated various aspects of central groupoids. Most importantly, Knuth found two models for central groupoids, one being a digraph model, the other being a model based upon the $\{0,1\}$–matrices that are the incidence matrices of these digraphs. The incidence matrices made an interesting contribution to a question posed by Hoffman in [Hof67]: which $\{0,1\}$–matrices A have the property that $A^2 = J$, where J is the matrix consisting entirely of ones?

In [Sha74] Shader demonstrates that non–natural central groupoids exists for all orders n^2, $n \geq 3$. The question of an exhaustive list of central groupoids, or equivalently an exhaustive list of matrices A with $A^2 = J$, remains open.

A digraph has the *unique path property* of length n UPP_n, if there is a unique path of length n between any two nodes [FAYF85, Men70]. For $n = 1$ we obtain complete graphs. If $(S, \cdot)$ is a central groupoid, then the digraph with node set S and edges $\{(a, a \cdot b) : a, b \in S\}$ is a UPP_2 graph. If (N, E) is a UPP_2 graph, then for every pair of nodes $a, b \in V$, there is a unique node c that is the midpoint of the unique path from a to b. Defining $a \circ b := c$ gives us a binary operation and $(V, \circ)$ is a central groupoid. Thus the determination of UPP_2 graphs and central groupoids is equivalent. If A is the incidence matrix of a UPP_2 graph, then $A^2 = J$ where J is the matrix consisting entirely of ones, so we have the solutions to Hoffman's problem.

Many investigations of this and related problems have been made, in particular looking at special classes of examples from circulant matrices[Rys70, Lam75, Lam77, LvL78, Wan80, Wan82, Ma84, YWH99].

4. Direct Implementation

This problem of determining all UPP_2 graphs seemed like an easy problem for an orderly algorithm approach. We proceeded as follows.

Let V be the set of directed edges in a graph of order n^2. Let G be the symmetric group on n^2 points acting upon these edges naturally. Let $P(X)$ be the property of a graph defined by the edges X having at most one path of length 2 between any pair of nodes. $\Theta(X)$ can be directly defined using the canonical labelling property described above on the graph induced by X.

We can remove many possible extensions using other properties of central groupoids; for instance we know (see below) that the in and out valency of each node in a UPP_2 graph is n. Thus we do not add edges between nodes that have already reached that limit.

Alhough the algorithm, when run on the problem for $n = 2$, terminates quickly with the correct answer, attempts (with lots of clever implementation tricks as suggested by Royle) for $n = 3$ ran for several weeks before we terminated them.

The problem seems to be that the number of stages in the algorithm is n^3. In the process of building partial solutions, many partial examples are constructed that cannot be extended to a full solution. It seems that the recursion depth n^3 allows a lot of extraneous and unproductive branching, bogging the process down and preventing the algorithm from working effectively.

Thus we resorted to a different approach. The structures that we introduce in the next section are generalisations of central groupoids, yet have a combinatorial structure that is somewhat simpler.

5. A Generalisation

Definition 5.1. *A* Semicentral Bigroupoid *is a* $(2,2)$*-algebra* $(S, \bullet, \circ)$ *satisfying the following axioms:*

$$(a \bullet b) \circ (b \bullet c) = b \tag{5.1}$$

$$(a \circ b) \bullet (b \circ c) = b \tag{5.2}$$

If $(S, \bullet)$ is a central groupoid, then $(S, \bullet, \bullet)$ is a semicentral bigroupoid, so this is a proper generalisation.

Note also that the definition is completely symmetric in $\bullet$ and $\circ$, i.e. $(S, \circ, \bullet)$ is a semicentral bigroupoid iff $(S, \bullet, \circ)$ is. The *dual* of a semicentral bigroupoid $(S, \bullet, \circ)$ is $(S, \circ, \bullet)$. It is often not necessary to prove results for both operations, as they carry across by duality.

Example 5.2. *Let* A,B *be two sets, and let* $Q = A \times B$. *Define*

$$(a_1, b_1) \bullet (a_2, b_2) = (a_1, b_2) \tag{5.3}$$

$$(a_1, b_1) \circ (a_2, b_2) = (a_2, b_1) \tag{5.4}$$

Then $(Q, \bullet, \circ)$ *is a semicentral bigroupoid.*

In the above, $(Q, \bullet)$ defines a rectangular semigroup. This corresponds to the natural central groupoids, in that it can be constructed as a "product of points" [Eva67], see also Lemma 5.7. Below we will see that it is the only associative semicentral bigroupoid.

Lemma 5.3. *Let* $(S, \bullet, \circ)$ *be a semicentral bigroupoid. Both the operations are anti-commutative, that is,* $a \bullet b = b \bullet a \Rightarrow a = b$ *and similarly for* $\circ$. *Also* $a \bullet a = a$ *iff* $a \circ a = a$, *thus* $(S, \bullet)$ *is idempotent iff* $(S, \circ)$ *is idempotent.*

These results follow by direct calculation. Note that anticommutative is a stronger condition than noncommutative. In the following, we will often omit $\bullet$ and represent the operation by juxtaposition where no confusion would result.

We can take any semicentral bigroupoid and "bend" it to get another semicentral bigroupoid. This method can be used to find new examples of semicentral bigroupoids.

Proposition 5.4. *If $(S, \bullet, \circ)$ is a semicentral bigroupoid, and $\phi : S \to S$ is a permutation of S, then the algebra $(S, *, +)$ with*

$$a * b = \phi^{-1}(a \bullet b) \tag{5.5}$$

$$a + b = \phi(a) \circ \phi(b) \tag{5.6}$$

is also a semicentral bigroupoid.

The calculation behind this result is mechanical. Note that the new semicentral bigroupoid will in general not be isomorphic to the old one; see Lemma 5.19.

Definition 5.5. *The* lifting of $(S, \bullet, \circ)$ by ϕ *is the algebra $(S, *, +)$ defined above. The* square map $\phi_\bullet$ *of $(S, \bullet, \circ)$ is $\phi_\bullet : x \mapsto x \bullet x$*

The square map, $\phi_\bullet : a \mapsto a \bullet a$ is a permutation:

$$\begin{aligned} \phi_\bullet(a) = \phi_\bullet(b) &\Rightarrow a \bullet a = b \bullet b \\ &\Rightarrow (a \bullet a) \circ (a \bullet a) = (b \bullet b) \circ (b \bullet b) \Rightarrow a = b \end{aligned} \tag{5.7}$$

If we lift by the square map then the derived operation $*$ is idempotent:

$$a * a = \phi_\bullet^{-1}(a \bullet a) = \phi_\bullet^{-1}\phi_\bullet(a) = a. \tag{5.8}$$

This will be referred to as the *idempotent lifting* of a semicentral bigroupoid. If we then lift the resulting idempotent semicentral bigroupoid by the permutation $\phi_\bullet^{-1}$ then we will obtain $(S, \bullet, \circ)$.

It is clear that the lifting operation is invertible and that every semicentral bigroupoid is the lifting of an idempotent semicentral bigroupoid by a permutation that becomes the inverse of the square map in the lifting.

That we can have any permutation as the square map in a semicentral bigroupoid, and thus any number of idempotents, is a contrast to the case for a central groupoid, where there are exactly $\sqrt{|S|}$ idempotents for S finite.

We see the following.

Proposition 5.6. *Every semicentral bigroupoid $(S, \bullet, \circ)$ can be uniquely represented as an idempotent semicentral bigroupoid and a permutation in $Symm(S)$. Conversely, every such pair gives a semicentral bigroupoid that is idempotent iff the permutation is trivial.*

In Proposition 5.18 we will see exactly when two semicentral bigroupoids are isomorphic, based upon the isomorphism of their idempotent representatives and relations between their square maps. We will focus upon idempotent semicentral bigroupoids for now.

Let's apply this to a central groupoid. As mentioned above, if $(S, \bullet)$ is a central groupoid, then $(S, \bullet, \bullet)$ is a semicentral bigroupoid. Take the example of the natural central groupoid of order 4. The elements are $\{aa, ab, ba, bb\}$ with operation $x_1x_2 \bullet x_3x_4 = x_2x_3$. The square map is the permutation $\phi_\bullet = (ab\ ba)$.

This is the permutation that reverses the entries in the product, i.e. $\phi_\bullet : xy \mapsto yx$. If we construct the multiplication tables for the lifting by $\phi_\bullet$, then we obtain the following:

$$\begin{array}{c|cccc} * & aa & ab & ba & bb \\ \hline aa & aa & aa & ba & ba \\ ab & ab & ab & bb & bb \\ ba & aa & aa & ba & ba \\ bb & ab & ab & bb & bb \end{array} \qquad \begin{array}{c|cccc} + & aa & ab & ba & bb \\ \hline aa & aa & ab & aa & ab \\ ab & aa & ab & aa & ab \\ ba & ba & bb & ba & bb \\ bb & ba & bb & ba & bb \end{array} \tag{5.9}$$

We see that this lifting is an idempotent semicentral bigroupoid, in fact an associative one.

In general one can make the following statement.

Lemma 5.7. *The idempotent lifting of a natural central groupoid is an associative semicentral bigroupoid.*

The proof is mechanical.

In Lemma 5.3 above, we saw that the operations in a semicentral bigroupoid are anticommutative. In [McL54], McLean shows that the only anticommutative semigroups are the rectangular semigroups. Thus if $(S, *, +)$ is a semicentral bigroupoid with $(S, *)$ associative, then $(S, *)$ is a rectangular semigroup, as is $(S, +)$, with a structure as in Example 5.2.

We "coordinatise" our algebra. An idempotent semicentral bigroupoid gives us a combinatorial structure. Define

$$\rho : S \to \mathcal{P}(S^2) \tag{5.10}$$

$$x \mapsto \{(ax, xb) | a, b \in S\} \tag{5.11}$$

Where $\mathcal{P}(X)$ denotes the power set of X.

Lemma 5.8. *$\rho(S) = \{\rho(s)|s \in S\}$ is a partition of S^2. For every $x \in S$ there exists $A, B \subseteq S$ such that*

- *$\rho(x) = A \times B$.*
- *$|A \cap B| = 1$.*
- *$B \circ A = S$.*
- *$A \circ B = \{x\}$*

The proof is mechanical calculation with $A = S \bullet x,\ B = x \bullet S$.

So the ρ map breaks S^2 down into a collection of cartesian products, *rectangles*, that form a partition. In this way we find a coordinatisation of S in terms of a pair of trivially intersecting sets; taking some $\rho(x) = A \times B$, every element s of S can be uniquely represented as a pair (a, b) with $b \circ a = s$.

Corollary 5.9. *Let $(S, \bullet, \circ)$ be a semicentral bigroupoid. If $a \circ b = c \circ d = x$, then $a \circ d = c \circ b = x$, and similarly for $\bullet$.*

Proof. By Lemma 5.8 above, $\rho(x) = A \times B$, $A = S \bullet x$, $B = x \bullet S$. Then

$$a = (a \circ a) \bullet (a \circ b) = (a \circ a) \bullet x \in Sx \tag{5.12}$$

similarly $c \in S \bullet x$, $b, d \in x \bullet S$. Then $A \circ B = (S \bullet x) \circ (x \bullet S) = \{x\}$, so

$$a \circ d \in A \circ B \;\Rightarrow\; a \circ d = x \tag{5.13}$$

$$c \circ b \in A \circ B \;\Rightarrow\; c \circ b = x \tag{5.14}$$

□

Such a property is seen also in the L–groupoids in [GR03].

Lets investigate the structure of this collection of sets.

Let $\mathcal{R}^\circ = \{(Sx, xS) | x \in S\}$ be a set of ordered pairs of sets. It is the set of "rectangles" in the table of $\circ$; Let $R^\circ_x = \{(a, b) | a \circ b = x\}$, then $\mathcal{R}^\circ = \{R^\circ_x | x \in S\}$.

What is the structure of this $\mathcal{R}^\circ$? First, it is a partition, so

$$\text{For all } (a, b) \in S^2 \; \exists! R = (R_1, R_2) \in \mathcal{R}^\circ \text{ s.t. } a \in R_1, b \in R_2. \tag{5.15}$$

This follows from Lemma 5.8 above. Then,

$$\text{For any pair of rectangles } Q, R \in \mathcal{R}^\circ, |Q_1 \cap R_2| = 1. \tag{5.16}$$

To see this, note that there are some $x, y \in S$ such that $Q_1 = S \bullet x, R_2 = y \bullet S$. If $a \in Q_1 \cap R_2$, then $a = b \bullet x = y \bullet c$ for some $b, c \in S$. Then by Corollary 5.9 above, $a = y \bullet x$, that is, $Q_1 \cap R_2 = \{y \bullet x\}$.

So we see that an idempotent semicentral bigroupoid $(S, \bullet, \circ)$ has the structure of a set of rectangles satisfying a pair of identities (5.15), (5.16). We now demonstrate that this connection is invertible, i.e. given a set of such rectangles one obtains an idempotent semicentral bigroupoid.

Definition 5.10. *A* Rectangular Structure *on a set S, called the* base set*, is a collection $\mathcal{R}$ of ordered pairs of subsets, called* rectangles*, of S, such that*

$$\forall (s, t) \in S^2 \; \exists! \; R \in \mathcal{R} \text{ such that } (s, t) \in R \tag{5.17}$$

$$\forall R, Q \in \mathcal{R}, |R_1 \cap Q_2| = 1 \tag{5.18}$$

where we identify $R = (R_1, R_2) = R_1 \times R_2$.

We say two rectangular structures are isomorphic *if there is an invertible map between the base sets that preserves rectangles.*

As an example, take two sets A, B. Define $S = A \times B$, and for all $(a, b) \in S$ define $R_{(a,b)} = (\{a\} \times B, A \times \{b\})$. Then

$$\mathcal{R} = \{R_{(a,b)} | a \in A, b \in B\} \tag{5.19}$$

is a rectangular structure on S. For any $((a, b), (c, d)) \in S^2$, we see that $((a, b), (c, d)) \in R_{(a,d)}$, and this is obviously unique. Let $R = R_{(a,b)}$, $Q = R_{(c,d)}$ be two rectangles in $\mathcal{R}$. Then $R_1 = \{a\} \times B$ and $Q_2 = A \times \{d\}$, so $|R_1 \cap Q_2| = |\{\{a\} \times \{d\}\}| = 1$.

Of course, every semicentral bigroupoid gives us a rectangular structure, as demonstrated above.

The *format* of a rectangle (A, B) is the ordered pair $(|A|, |B|)$.

Proposition 5.11. *If $\mathcal{R}$ is a rectangular structure with base set S, and $R = (R_1, R_2) \in \mathcal{R}$ is some rectangle, then $|R_1||R_2| = |S| = |\mathcal{R}|$. Moreover, for any other rectangle $Q = (Q_1, Q_2) \in \mathcal{R}$, $|R_1| = |Q_1|$, i.e. all rectangles have the same format.*

Proof. Define the map:

$$d : \mathcal{R} \rightarrow S \tag{5.20}$$

$$R \mapsto r \text{ where } \{r\} = R_1 \cap R_2 \tag{5.21}$$

This map is well defined since for every $R \in \mathcal{R}$, $|R_1 \cap R_2| = 1$ by (5.18) above, so $R_1 \cap R_2 = \{r\}$ for some unique r.

By (5.17) above, (r, r) is in a unique rectangle, so this map is bijective and $|\mathcal{R}| = |S|$.

For some fixed rectangle $R \in \mathcal{R}$ define:

$$r_R : \mathcal{R} \rightarrow R_2 \times R_1 \tag{5.22}$$

$$Q \mapsto (Q_1 \cap R_2, Q_2 \cap R_1) \tag{5.23}$$

where $(\{a\}, \{b\})$ and (a, b) are equated to simplify notation. Suppose $r_R(Q) = r_R(P) = (a, b)$ for some $P, Q \in \mathcal{R}$. Then $a \in P_1, Q_1$ and $b \in P_2, Q_2$, i.e. $(a, b) \in P, Q$, so by the uniqueness in (5.17) $P = Q$ and r_R is injective. (5.17) also forces surjectivity since for every $(s, t) \in R$, there is some $Q \in \mathcal{R}$ with $(t, s) \in Q$. Thus r_R is a bijection and $|R| = |R_1||R_2| = |\mathcal{R}|$.

Fix $s \in S$ and define

$$\mathcal{Q} = \{Q \in \mathcal{R} | s \in Q_1\}. \tag{5.24}$$

Take a rectangle $R \in \mathcal{R}$, for all $Q \in \mathcal{Q}$, $|Q_2 \cap R_1| = 1$. Thus the mapping

$$\mathcal{Q} \rightarrow R_1 \tag{5.25}$$

$$Q \mapsto q \text{ where } \{q\} = Q_2 \cap R_1 \tag{5.26}$$

is well–defined. For any $Q, T \in \mathcal{Q}$,

$$t \in Q_2 \cap T_2 \neq \emptyset \Rightarrow (s, t) \in Q, (s, t) \in T \Rightarrow Q = T \tag{5.27}$$

Thus the mapping is injective. Since for every $t \in R_1$, there is some $Q \in \mathcal{R}$ such that $(s, t) \in Q$, the mapping is surjective, thus bijective, giving $|R_1| = |\mathcal{Q}|$. Since $\mathcal{Q}$ is independent of R, $|R_1|$ is thus fixed, as is $|R_2|$, for all rectangles $R \in \mathcal{R}$. □

A rectangular structure $\mathcal{R} = \{A_i \times B_i\}$ is *right (left) partitioned* if the sets B_i (A_i) form a partition of S. If it is partitioned on both sides, we call it doubly partitioned.

If $(S, *, +)$ is a semicentral bigroupoid then $\mathcal{R}^*$ is left partitioned iff $\mathcal{R}^+$ is right partitioned (and vice versa).

From a rectangular structure $\mathcal{R}$, using the bijection d from equation (5.20) above and denoting by $R(s,t)$ the unique rectangle on the pair (s,t) guaranteed by (5.17), define

$$\begin{aligned} \bullet : S \times S &\to S \\ (s,t) &\mapsto u \text{ where } \{u\} = (d^{-1}(s))_2 \cap (d^{-1}(t))_1 \end{aligned} \tag{5.28}$$

$$\begin{aligned} \circ : S \times S &\to S \\ (s,t) &\mapsto d(R(s,t)) \end{aligned} \tag{5.29}$$

as binary operations on S.

Proposition 5.12. *The algebra $(S, \bullet, \circ)$, with operations defined as in (5.28),(5.29) above, is an idempotent semicentral bigroupoid.*

Proof.

$$(a \bullet b) \circ (b \bullet c) = (d^{-1}(a)_2 \cap d^{-1}(b)_1) \circ (d^{-1}(b)_2 \cap d^{-1}(c)_1) \tag{5.30}$$

$$= k \circ l \text{ for some } k, l \in S \tag{5.31}$$

$$= d(R(k,l)) \tag{5.32}$$

But $k \in (d^{-1}(b))_1$ and $l \in (d^{-1}(b))_2$. Then $(k,l) \in d^{-1}b$, thus $R(k,l) = d^{-1}b$, thus $k \circ l = d(R(k,l)) = b$.

Now for the dual.

$$(a \circ b) \bullet (b \circ c) = d(R(a,b)) \bullet d(R(b,c)) \tag{5.33}$$

$$= d^{-1}(d(R(a,b)))_2 \cap d^{-1}(d(R(b,c)))_1 \tag{5.34}$$

$$= R(a,b)_2 \cap R(b,c)_1 \tag{5.35}$$

Since $b \in R(a,b)_2$, $b \in R(b,c)_1$ and their intersection is unique,

$$R(a,b)_2 \cap R(b,c)_1 = \{b\}. \tag{5.36}$$

Thus the two axioms of a semicentral bigroupoid are satisfied. Since $a \circ a = d(R(a,a)) = a$ for all $a \in S$ we see that the $\circ$ operation is idempotent, thus by Lemma 5.3 both operations are idempotent. $\square$

If we call the format of an operation table the format of the derived rectangular structure, we get the following.

Corollary 5.13. *If $(S, \bullet, \circ)$ is a semicentral bigroupoid with format (a,b) for the $\bullet$ operation table, then the format of the $\circ$ operation table is (b,a).*

Proof. Let (c,d) be the format of the $\circ$ operation table. For any $x \in S$, $\rho(x) = S \bullet x \times x \bullet S$ is the rectangle filled with x in the $\circ$ operation table. Thus $d = |x \bullet S|$, so there are d rectangles in the x row of the $\bullet$ operation table, all of which have the same format (a, b). Thus $db = |S|$. But $|S| = ab$ so $a = d$. Similarly $b = c$, i.e. the format of the $\circ$ operation table is (b, a). $\square$

Corollary 5.14 ([Eva67] Theorem 1)**.** *A finite central groupoid* $(S, \bullet)$ *has square order.*

Proof. If $(S, \bullet)$ is a central groupoid, then $(S, \bullet, \bullet)$ is a semicentral bigroupoid. Thus the formats of the operations are (a, b) and (b, a), but these are identical, so $a = b$ and $|S| = ab = a^2$. $\square$

We now investigate the isomorphism of semicentral bigroupoids.

Lemma 5.15. *If* $(S, \bullet, \circ)$ *and* $(T, +, *)$ *are semicentral bigroupoids and* ϕ *is an isomorphism from* $(S, \bullet)$ *to* $(T, +)$*, then* ϕ *is also an isomorphism from* $(S, \circ)$ *to* $(T, *)$*.*

Proof. We use a coordinatisation argument. Note first that

$$\{a \circ b\} = \{x | y \bullet x = a\} \cap \{x | x \bullet y = b\} \tag{5.37}$$

$$\{a * b\} = \{x | y + x = a\} \cap \{x | x + y = b\} \tag{5.38}$$

Then compute:

$$\begin{aligned} \{\phi(a \circ b)\} &= \{\phi x | y \bullet x = a\} \cap \{\phi x | x \bullet y = b\} && (5.39) \\ &= \{\phi x | \phi y + \phi x = \phi a\} \cap \{\phi x | \phi x + \phi y = \phi b\} && (5.40) \\ &= \{x | y + x = \phi a\} \cap \{x | x + y = \phi b\} && (5.41) \\ &= \{\phi a * \phi b\} && (5.42) \end{aligned}$$

so ϕ is a $\circ$–morphism, and we are done. $\square$

Thus in order to show that a mapping ϕ on semicentral bigroupoid S is an isomorphism we need to show it for one operation, the other follows automatically. Note that the above argument does not work for general morphisms.

We have seen that every semicentral bigroupoid is a lifting of an idempotent one. We also have:

Lemma 5.16. *Every semicentral bigroupoid* $(S, \bullet, \circ)$ *has an associated rectangular structure that is constant across liftings.*

Proof. Suppose $(S, *, +)$ is a lifting of $(S, \bullet, \circ)$ by ϕ. Define the rectangular structures as follows:

$$R^\bullet_x = \{(a, b) | a \bullet b = x\}, \quad R^*_x = \{(a, b) | a * b = x\} \tag{5.43}$$

$$\mathcal{R}^\bullet = \{R^\bullet_x | x \in S\}, \quad \mathcal{R}^* = \{R^*_x | x \in S\} \tag{5.44}$$

These are rectangular structures as they are derived from semicentral bigroupoids.

Take $(a,b),(c,d) \in R \in \mathcal{R}^\bullet$, two pairs in some rectangle. Thus $a \bullet b = c \bullet d = x$ for some $x \in S$. But $a * b = \phi^{-1}(a \bullet b) = \phi^{-1}(c \bullet d) = c * d$ so (a,b) and (c,d) are in the same rectangle in $\mathcal{R}^*$. Thus the rectangular structures are the same for both semicentral bigroupoids. $\square$

Proposition 5.17. *Two idempotent semicentral bigroupoids are isomorphic iff the associated rectangular structures are isomorphic.*

Proof. ($\Rightarrow$) Let the semicentral bigroupoids be $(S, \bullet, \circ)$ and $(T, *, +)$, with isomorphism $\beta : S \to T$. Take $\mathcal{R}^\bullet, \mathcal{R}^*$ as above, and take $R \in \mathcal{R}^\bullet$. Then

$$\beta(R) = \{(\beta a, \beta b) | (a,b) \in R\} \tag{5.45}$$

$$= \{(\beta a, \beta b) | a \bullet b = x\} \text{ for some } x \in S \tag{5.46}$$

$$= \{(\beta a, \beta b) | \beta a * \beta b = \beta(a \bullet b) = \beta(x)\} \tag{5.47}$$

$$= \{(a,b) | a * b = \beta x\} \tag{5.48}$$

which is a rectangle in $\mathcal{R}^*$. Similarly one shows that $\beta^{-1} : T \to S$ respects rectangles, so β is a rectangular structure isomorphism.

($\Leftarrow$) Take two idempotent semicentral bigroupoids $(S, \bullet, \circ)$ and $(T, *, +)$, and suppose $\beta : S \to T$ preserves the rectangles of the associated rectangular structures $\mathcal{R}^\bullet, \mathcal{R}^*$. Take some $a, b \in S$. Then $a \bullet b = x = x \bullet x$ for some x. Thus (a,b) and (x,x) are in the same rectangle in $\mathcal{R}^\bullet$, and thus $(\beta a, \beta b)$ and $(\beta x, \beta x)$ are in the same rectangle in $\mathcal{R}^*$. Thus

$$\beta(a) * \beta(b) = \beta(x) * \beta(x) = \beta(x) = \beta(a \bullet b) \tag{5.49}$$

so β is an isomorphism of the algebras. $\square$

The construction of a rectangular structure from a semicentral bigroupoid above and the reverse construction in Proposition 5.12 are complementary in that given an idempotent semicentral bigroupoid $(S, *, +)$, the semicentral bigroupoid $(S, \bullet, \circ)$ derived from the associated rectangular structure is the same, i.e. $a * b = a \bullet b$, $a + b = a \circ b$.

Rectangular structures and idempotent semicentral bigroupoids are essentially equivalent.

Note also that the forward implication in the proposition above does not use the idempotence, so we know that isomorphic semicentral bigroupoids have isomorphic rectangular structures in all cases.

Now to look at a similar result for non–idempotent semicentral bigroupoids.

Proposition 5.18. *Two semicentral bigroupoids $(S, \bullet, \circ)$ and $(T, *, +)$ are isomorphic, with isomorphism $\beta : S \to T$, iff their idempotent liftings are isomorphic by β, and $\beta\phi_\bullet = \phi_*\beta$ for the square maps $\phi_\bullet$ and ϕ_*.*

Proof. In this proof, I will use the symbol $\bar{\bullet}$ for the idempotent lifting of the $\bullet$ operation, i.e. $a\bar{\bullet}b = \phi_\bullet^{-1}(a \bullet b)$.

($\Rightarrow$) We know from the forward half of Proposition 5.17 above that the rectangular structures are isomorphic, thus the idempotent semicentral bigroupoids generated from the rectangular structures are isomorphic by some bijection β.

Now for all $a, b \in S$:

$$\begin{aligned}
\beta(a\bar{\bullet}b) &= \beta(\phi_\bullet^{-1}(a \bullet b)) && (5.50)\\
\text{and } \beta(a\bar{\bullet}b) &= \beta(a)\bar{*}\beta(b) && (5.51)\\
&= \phi_*^{-1}(\beta(a) * \beta(b)) && (5.52)\\
&= \phi_*^{-1}(\beta(a \bullet b)) && (5.53)\\
\text{thus } \phi_*^{-1}\beta &= \beta\phi_\bullet^{-1} && (5.54)\\
\Rightarrow \beta\phi_\bullet &= \phi_*\beta && (5.55)
\end{aligned}$$

($\Leftarrow$) The converse follows directly by computation.

$$\begin{aligned}
\beta(a \bullet b) &= \beta\phi_\bullet\phi_\bullet^{-1}(a \bullet b) && (5.56)\\
&= \phi_*\beta(a\bar{\bullet}b) && (5.57)\\
&= \phi_*(\beta(a)\bar{*}\beta(b)) && (5.58)\\
&= \phi_*\phi_*^{-1}(\beta(a) * \beta(b)) && (5.59)\\
&= \beta(a) * \beta(b) && (5.60)
\end{aligned}$$

So β is a semicentral bigroupoid isomorphism. □

For the following, S_S is the symmetric group on S, $Symm_{RS}(S)$ is the symmetry group of the rectangular structure of $(S, \bullet, \circ)$, and $[a, b]$ is the commutator of a and b.

Lemma 5.19. *A lifting of a semicentral bigroupoid $(S, \bullet, \circ)$ by ϕ is an isomorphism iff $\phi \in [\phi_\bullet, Symm_{RS}(S)]$*

Proof. The square map in the lifting $(S, *, +)$ is

$$\phi_*(x) = x * x = \phi^{-1}(x \bullet x) = \phi^{-1}\phi_\bullet(x) \quad (5.61)$$

We know that rectangular structures are preserved by lifting (Lemma 5.16), so we need only look at the second condition in the last proposition.

The lifting is isomorphic, with isomorphism α, if α is an automorphism of the rectangular structure associated with S and

$$\begin{aligned}
\alpha\phi_\bullet &= \phi_*\alpha && (5.62)\\
\Leftrightarrow \alpha\phi_\bullet &= \phi^{-1}\phi_\bullet\alpha && (5.63)\\
\Leftrightarrow \phi &= \phi_\bullet\alpha\phi_\bullet^{-1}\alpha^{-1} && (5.64)\\
\text{that is, } \phi &\in [\phi_\bullet, Symm_{RS}(S)] && (5.65)
\end{aligned}$$

□

Proposition 5.20. *Two liftings of an idempotent semicentral bigroupoid by $\phi, \bar{\phi}$ are isomorphic iff the $\phi, \bar{\phi}$ are conjugate by an element from $Symm_{RS}(S)$.*

Proof. Let $(S_1, \bullet_1, \circ_1)$(resp. $(S_2, \bullet_2, \circ_2)$) be the lifting by ϕ (resp. $\bar{\phi}$), that is

$$a \bullet_1 b = \phi^{-1}(a \bullet b) \tag{5.66}$$

$$a \bullet_2 b = \bar{\phi}^{-1}(a \bullet b) \tag{5.67}$$

Note that $\phi_{\bullet_1}(x) = x \bullet_1 x = \phi^{-1}(x \bullet x) = \phi^{-1}(x)$ so $\phi_{\bullet_1} = \phi^{-1}$, similarly $\phi_{\bullet_2} = \bar{\phi}^{-1}$.

S_2 is a lifting of S_1 by $(\phi^{-1}\bar{\phi})$,

$$a \bullet_2 b = \bar{\phi}^{-1}(a \bullet b) \tag{5.68}$$

$$= \bar{\phi}^{-1}\phi(a \bullet_1 b) \tag{5.69}$$

$$= (\phi^{-1}\bar{\phi})^{-1}(a \bullet_1 b) \tag{5.70}$$

Thus $\alpha \in Symm_{RS}(S)$ is an isomorphism $S_1 \to S_2$

$$\Leftrightarrow \phi^{-1}\bar{\phi} = \phi_{\bullet_1}\alpha\phi_{\bullet_1}^{-1}\alpha^{-1} \tag{5.71}$$

$$= \phi^{-1}\alpha\phi\alpha^{-1} \tag{5.72}$$

$$\Leftrightarrow \bar{\phi} = \alpha\phi\alpha^{-1} \tag{5.73}$$

i.e. iff ϕ and $\bar{\phi}$ are conjugate by an element of $Symm_{RS}(S)$. □

We generalise the UPP_2 condition as follows. Take a fixed set of vertices, and look at two directed graphs on this set, G_R and G_B. Call these as the red and blue graphs respectively. The problem is to arrange these graphs such that, when we superimpose them, obtaining a multigraph, there is a unique directed path of length 2 coloured blue–red between any two nodes, and a unique directed path coloured red–blue. We refer to these as *symmetric unique 2–coloured 2–path graphs*. We must allow (in general) that two edges of differing colours exist between the same vertex pair. Thus we should speak of multigraphs. Thus the class of multigraphs might be termed *symmetric 2–coloured unique 2–path multigraphs*.

It is not known whether these are of any independent interest.

We note that the incidence matrices of these graphs have the property that $AB = BA = J$ where A, B are the incidence matrices of the two graphs and J is the matrix consisting of all 1s. These are generalisations of the matrices introduced by Hoffman in [Hof67].

Example 5.21 (Construction). *Take a semicentral bigroupoid, define coloured edges $a \to_{blue} b$ and $a \to_{red} b$ by*

$$a \to_{red} b \Leftrightarrow a \bullet c = b \ \exists c \tag{5.74}$$

$$a \to_{blue} b \Leftrightarrow a \circ c = b \ \exists c \tag{5.75}$$

Conversely, given a graph pair define a semicentral bigroupoid as follows. Let S be the vertex set of the graphs. For any $a, b \in S$, let c_r, c_b be the unique vertices on the paths between a and b:

$$a \to_{red} c_r \to_{blue} b \tag{5.76}$$

$$a \to_{blue} c_b \to_{red} b \tag{5.77}$$

Define

$$a \bullet b = c_r \tag{5.78}$$

$$a \circ b = c_b \tag{5.79}$$

and we have an $(2, 2)$–algebra $(S, \bullet, \circ)$.

Proposition 5.22. *If $(S, \bullet, \circ)$ is a semicentral bigroupoid, then the construction above determines a symmetric 2–coloured unique 2–path multigraph. Similarly, given a symmetric 2–coloured unique 2–path multigraph, the construction above defines a semicentral bigroupoid. The constructions are inverses of one another.*

The proof is mechanical.

Note that if some element a is idempotent, then $a \bullet a = a$ so there is a red loop arc on the node a, similarly a blue loop arc. Thus if S is idempotent, every node is a loop node.

Consider two categories, $\mathcal{S}$ of semicentral bigroupoids, and $\mathcal{G}$ of symmetric 2–coloured unique 2–path multigraphs. Consider the functor from $\mathcal{S}$ to $\mathcal{G}$ as described in Example 5.21 above, and take an exact sequence $A \to_f B \to_g C$ in $\mathcal{S}$. Since the mappings f, g operate on elements of the semicentral bigroupoids, they operate on vertices of the graphs under the functor, carrying arcs across with them. Thus $range(f) = ker(g)$ in $\mathcal{G}$, so the functor is exact. Thus we get the result:

Lemma 5.23. *Isomorphic semicentral bigroupoids give isomorphic multigraph pairs by the construction in Example 5.21 above.*

Thus the correspondence between multigraph pairs and semicentral bigroupoids is an equivalence. The following shows that the automorphism group of a semicentral bigroupoid can be obtained using the automorphism groups of the associated graphs.

Lemma 5.24. *If G_b, G_r are the graphs defined by a semicentral bigroupoid S, then*

$$Aut(S) = Aut(G_b) \cap Aut(G_r) \tag{5.80}$$

Proof. Note that automorphisms are already bijections.

($\subseteq$): Take $\phi \in Aut(S)$. Take any red edge $a \rightarrow_{red} b$, so there is some c such that $a \bullet c = b$.

$$\phi a \bullet \phi c = \phi(a \bullet c) = \phi b \tag{5.81}$$

So $\phi a \rightarrow_{red} \phi b$, so $\phi \in Aut(G_r)$. Similarly $\phi \in Aut(G_b)$ and we are done.

($\supseteq$): Take some $\phi \in Aut(G_b) \cap Aut(G_r)$, $a, b \in S$ and $c = a \bullet b$ so $a \rightarrow_{red} c \rightarrow_{blue} b$. Then

$$\phi \in Aut(G_r) \quad \Rightarrow \quad \phi a \rightarrow_{red} \phi c \tag{5.82}$$

$$\phi \in Aut(G_b) \quad \Rightarrow \quad \phi c \rightarrow_{blue} \phi b \tag{5.83}$$

Then by uniqueness of the path

$$\phi a \rightarrow_{red} (\phi a \bullet \phi b) \rightarrow_{blue} \phi b \tag{5.84}$$

$$\phi a \rightarrow_{red} (\phi a) \bullet (\phi b) \rightarrow_{blue} \phi b \tag{5.85}$$

we know that $\phi c = \phi(a \bullet b) = \phi a \bullet \phi b$ and similarly $\phi(a \circ b) = \phi a \circ \phi b$ so $\phi \in Aut(S)$ and we are done. $\square$

If we look at idempotent semicentral bigroupoids, then the associated multigraph pairs have loop edges of both colours on each node. However they do not have any other repeated edges. We can then ignore the loop edges for determining the automorphism groups and other such properties.

6. Applications to Central Groupoids

We see that the semicentral bigroupoids have a lot of structure. What does this mean for central groupoids.

We have already seen that the format of a central groupoid must be $n \times n$. A central groupoid is a lifting of a square idempotent semicentral bigroupoid by a permutation. Let ϕ be this permutation. By the central groupoid axiom, $(a \cdot a) \cdot (a \cdot a) = a$, but this is also $(a \cdot a) \cdot (a \cdot a) = \phi\phi a = a$ so ϕ is of order 2.

Lemma 6.1. *If $(S, +, *)$ is an idempotent semicentral bigroupoid with $\phi : (S, +) \rightarrow (S, *)$ an isomorphism of order 2, then the lifting of S by ϕ is a central groupoid.*

Proof. Let $(S, \bullet, \circ)$ be the lifting of $(S, +, *)$ by ϕ. We know that

$$\begin{aligned} a \bullet b &= \phi(a + b) \\ a \circ b &= \phi a * \phi b \end{aligned}$$

By the isomorphism property of ϕ then $a \bullet b = \phi(a + b) = \phi a * \phi b = a \circ b$ so $(S, \bullet, \bullet)$ is a semicentral bigroupoid so $(S, \bullet)$ is a central groupoid. $\square$

The two graphs defined above from a semicentral bigroupoid are defined by the operations $+$ and $*$, so this means that the two graphs are isomorphic with isomorphism ϕ.

If the rectangular structure underlying a central groupoid is partitioned, then the partitions are apparent on one side of the multiplication table of $*$ but on the other side of the multiplication table of $+$. However these operations are isomorphic, so if the rectangular structure is partitioned, then it must be partitioned on both sides.

Lemma 6.2. *If S is a square associative semicentral bigroupoid then there is only one central groupoid lifting of it and it is the natural central groupoid.*

Proof. The automorphisms of a rectangular semigroup $S = A \times B$ are direct products of permutations of A and B. (find a reference for this)

Let $(S, +, *)$ be an associative semicentral bigroupoid of format $n \times n$. If ϕ is an isomorphism of $(S, +)$ onto $(S, *)$, then since the map $\sigma : (a, b) \mapsto (b, a)$ is also such an isomorphism, then the composition $\sigma\phi$ is an automorphism of the rectangular semigroup $(S, *)$. Thus $\phi(a, b) = (\phi_1 b, \phi_2 a)$ for some permutations ϕ_1, ϕ_2 of A.

Let ϕ and ψ be two permutations of S giving central groupoid liftings. We know that ϕ and ψ have n fixed points and $\frac{n^2-2}{2}$ swaps, so all of $\phi_1, \phi_2, \psi_1, \psi_2$ must have the same structure. Thus there are permutations α_1, α_2 of A such that $\phi_1^{\alpha_1} = \psi_1$ and $\phi_2^{\alpha_2} = \psi_2$. Since (α_1, α_2) is an isomorphism of S, we know that the liftings by ϕ and ψ are isomorphic using Prop 5.20.

It is clear that the lifting of S by σ is the natural central groupoid. □

Given a square rectangular structure $\mathcal{R}$, we can determine whether a central groupoid can be defined from it as follows:

- if $\mathcal{R}$ is partitioned, it must be partitioned on both sides. Which means it must be the rectangular structure made by products of points, and the only central groupoid that can be obtained from it is the natural one.
- The graph pair generated from $\mathcal{R}$ must be isomorphic.
- The set of isomorphisms can then be reduced to those of order 2. These are the candidate liftings for the central groupoid.
- These candidates are then separated into orbits under the conjugation operation by the automorphism group of the rectangular structure. Each orbit gives us one central groupoid, and all such central groupoids are nonisomorphic.

7. Generating and Filtering Process

In this section we outline the techniques that we used to obtain exhaustive enumerations of rectangular structures and to then filter out the appropriate examples for the construction of central groupoids.

Definition 7.1. *For positive integers n, m, an $n \times m$* rectangle *is a pair of sets (R_1, R_2) with $|R_1| = n, |R_2| = m$, $R_i \subset \{1, \ldots, (nm)\}$, $|R_1 \cap R_2| = 1$*

For instance $(\{1,4\},\{1,2,3,5\}),\ (\{1,2\},\{2,3,4,5\})$ are examples of 2×4 rectangles.

Definition 7.2. *A* $n\times m$ Partial Rectangular Structure P *is a collection of* $n\times m$ *rectangles such that*

- *For all* $Q,R\in P, |Q_1\cap R_2|=1$
- *For all* $a,b\in\{1,\dots,nm\}$ *there is at most one* $R\in P$ *such that* $a\in R_1, b\in R_2$.

One can easily see that a rectangular structure is a partial rectangular structure. Partial rectangular structures generalise rectangular structures with regard to the covering requirement (equation (5.17)). A *full* partial rectangular structure is one with nm rectangles. This is a rectangular structure.

We can obtain a graph pair from a partial rectangular structure in the same way as we obtain it from a rectangular structure.

We can combine the two graphs into one graph, the isomorphism of two graph pairs being equivalant to the isomorphism of two combined graphs.

A direct method is to generate a graph from the graph pair by having a coloured graph on n nodes. We colour the edges depending upon which graph they come from. We do not get repeated edges, so this is well defined. However GRAPE does not allow us to pass colourings to the graph automorphism test, so we have to use a more intricate method.

If the graph pair is A, B on node set $\{1,\dots,n\}$, then using the labels a and b we construct a graph with nodes

$$\{(a,x),(b,x)|x\in\{1,\dots,n\}\} \tag{7.1}$$

and edges

$$\begin{aligned}
&\{((a,x),(a,y))|(x,y)\in Edges(A)\}\cup\\
&\{((b,x),(b,y))|(x,y)\in Edges(B)\}\cup\\
&\{((a,x),(b,x))|x\in\{1,\dots,n\}\}\}\cup\\
&\{((a,x),(a,x))|x\in\{1,\dots,n\}\}\}
\end{aligned} \tag{7.2}$$

It is easy to see that the graphs constructed from two graph pairs are isomorphic iff the graph pairs are isomorphic. More importantly, the canonical labelling property of nauty, accessed via GRAPE, can be used on this graph. This is a canonical embedding, as defined above. .

Our situation is as follows. The set V is the set of $n\times m$ rectangles. P is the property of being a partial rectangular structure. We want to find the set T_{nm} of full partial rectangular structures, i.e. rectangular structures.

Note that we assemble only rectangles extending a given PRS that will satisfy P. We never construct the complete set of all rectangles, only those that are posible extensions, with a given middle.

We define Θ as in Corollary 2.6. We label rectangles R by their *middle*, the unique element $m(R) \in R_1 \cap R_2$. Then the map $F_{\mathcal{R}}(R)$ where $\mathcal{R}$ is a partial rectangular structure and $R \in \mathcal{R}$, takes R to the node labelled with $(a, m(R))$ in the graph defined above.

Initially we used the combinatorial values $v_1(\mathcal{R}, R) = |\{Q \in \mathcal{R} : m(R) \in Q_1\}|$ and $v_2(\mathcal{R}, R) = |\{Q \in \mathcal{R} : m(R) \in Q_2\}|$. The addition of a measure of intersection numbers, the ordered pair of multisets

$$v_3(\mathcal{R}, R) = (\{|R_1 \cap Q_1| : Q \in \mathcal{R}\}, \{|R_2 \cap Q_2| : Q \in \mathcal{R}\})$$

reduced computation time from 6 hours to 39 minutes.

8. Results

We have run the algorithms for examples up to order 10. Here we are only interested in the case of orders 4 and 9. For order 4 we obtain three rectangular structures, one doubly partitioned and two partitioned. Thus only the one (natural) central groupoid can be obtained. The order 9 search ran in a little over 39 minutes, drastically faster than the algorithm we attempted earlier. There are 184 rectangular structures of order 9.

We proceeded as follows. We filtered the partitioned rectangular structures out, leaving 67 examples. We then constructed the graph pairs and found only 7 pairs with isomorphic graphs. Of these, three had no isomorphisms of order 2, so they could be immediately excluded. For a further two examples, we found a unique isomorphism of order 2.

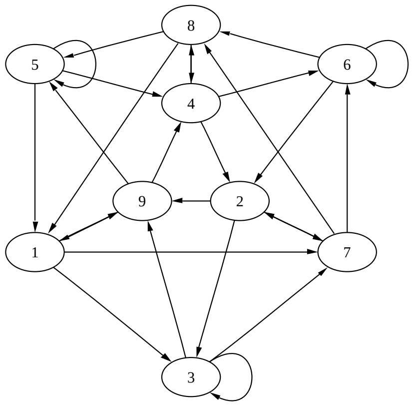
The remaining two rectangular structures both had two isomorphisms of order 2. Thus we obtained the automorphism group of the rectangular structure and determined the orbits of these permutations under the group of automorphisms by conjugation, as described in Proposition 5.20 above. For one example, both permutations were in the same orbit, so they give isomorphic liftings. In the other example, both permutations were fixed by the automorphism group. Thus they lead to nonisomorphic liftings, i.e. nonisomorphic central groupoids.

The doubly partitioned rectangular structure has only one central groupoid lifting, the natural one. Thus we obtained a total of one natural and 5 unnatural central groupoids of order 9, in accordance with the results in [CDLP03].

The numbers in the following refer to the indices in the list of rectangular structures obtained. The data is available from the author. The last two examples can be seen to arise from the same rectangular structure. Note that they have rather distinct graph structures, regardless of the common origin.

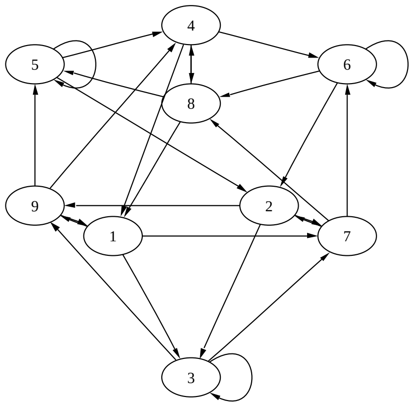
•	1	2	3	4	5	6	7	8	9
1	9	7	3	9	9	7	3	7	3
2	9	7	3	9	9	7	3	7	3
3	9	7	3	9	9	7	3	7	3
4	8	6	2	8	8	6	2	6	2
5	5	4	1	5	5	4	1	4	1
6	8	6	2	8	8	6	2	6	2
7	8	6	2	8	8	6	2	6	2
8	5	4	1	5	5	4	1	4	1
9	5	4	1	5	5	4	1	4	1

Natural central groupoid



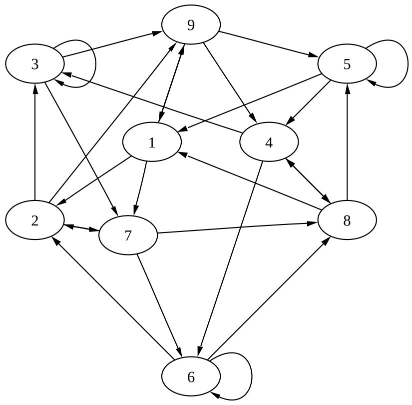
•	1	2	3	4	5	6	7	8	9
1	9	7	3	9	9	7	3	7	3
2	9	7	3	9	9	7	3	7	3
3	9	7	3	9	9	7	3	7	3
4	8	6	1	8	8	6	1	6	1
5	4	5	2	5	5	4	2	4	2
6	8	6	2	8	8	6	2	6	2
7	8	6	2	8	8	6	2	6	2
8	4	5	1	5	5	4	1	4	1
9	4	5	1	5	5	4	1	4	1

Number: 10 Lifting (1,9)(2,7)(4,8)

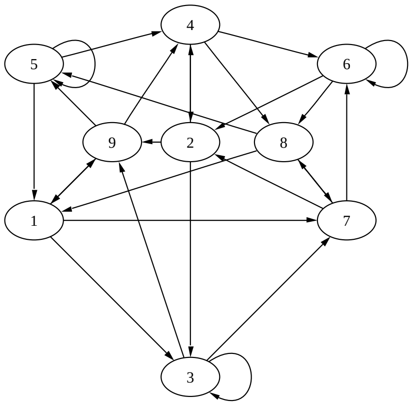


•	1	2	3	4	5	6	7	8	9
1	9	7	2	9	9	7	2	7	2
2	9	7	3	9	9	7	3	7	3
3	9	7	3	9	9	7	3	7	3
4	8	6	3	8	8	6	3	6	3
5	5	1	4	5	5	4	1	4	1
6	8	6	2	8	8	6	2	6	2
7	8	6	2	8	8	6	2	6	2
8	5	1	4	5	5	4	1	4	1
9	5	1	4	5	5	4	1	4	1

Number: 36 Lifting (1,9)(2,7)(4,8)

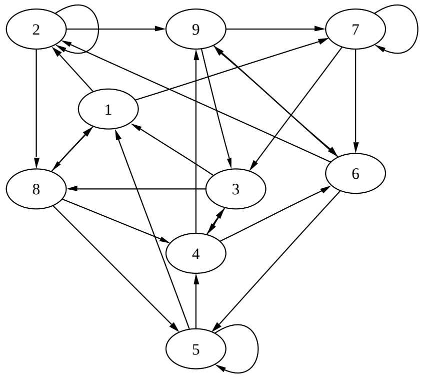


•	1	2	3	4	5	6	7	8	9
1	9	7	3	9	9	7	3	7	3
2	9	4	3	9	9	4	3	4	3
3	9	7	3	9	9	7	3	7	3
4	8	6	2	2	8	6	8	6	2
5	5	4	1	5	5	4	1	4	1
6	8	6	2	2	8	6	8	6	2
7	8	6	2	2	8	6	8	6	2
8	5	7	1	5	5	7	1	7	1
9	5	4	1	5	5	4	1	4	1



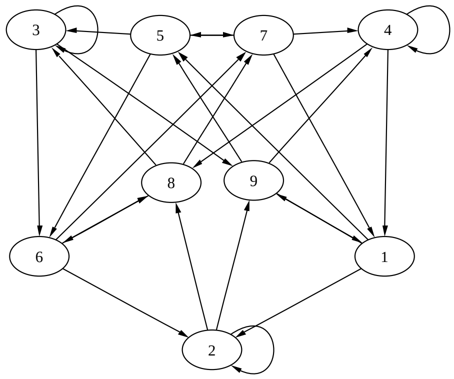
Number: 105 Lifting(1,9)(2,4)(7,8)

•	1	2	3	4	5	6	7	8	9
1	8	2	7	8	8	7	7	2	2
2	8	2	9	8	8	9	9	2	2
3	8	1	4	8	8	4	1	1	4
4	3	6	9	3	6	9	9	3	6
5	5	1	4	5	5	4	1	1	4
6	5	2	9	5	5	9	9	2	2
7	3	6	7	3	6	7	7	3	6
8	5	1	4	5	5	4	1	1	4
9	3	6	7	3	6	7	7	3	6



Number: 118 Lifting (1,8)(3,4)(6,9)

•	1	2	3	4	5	6	7	8	9
1	9	2	5	9	9	5	5	2	2
2	9	2	8	9	9	8	8	2	2
3	9	6	3	9	9	3	6	6	3
4	4	1	8	4	1	8	8	4	1
5	7	6	3	7	7	3	6	6	3
6	7	2	8	7	7	8	8	2	2
7	4	1	5	4	1	5	5	4	1
8	7	6	3	7	7	3	6	6	3
9	4	1	5	4	1	5	5	4	1



Number: 118 Lifting (1,9)(5,7)(6,8)

9. Conclusion

We have been able to use the techniques of orderly algorithms in order to enumerate the central groupoids of order 4 and 9. It was apparently necessary to move to a more general, but combinatorially and computationally more amenable structure, in order to be able to apply the technique fruitfully. The combinatorial rectangular structure was able to be assembled in n^2 stages instead of n^3, which may have suitably reduced the number of dead–end branches in the generation tree. The results connecting back to the structure of central groupoids were then necessary in order to be able to make the filtering process efficient.

The important results were the equivalence of idempotent semicentral bigroupoids and rectangular structures (Proposition 5.12) and the isomorphism of different liftings (Proposition 5.20). Thus we were able to determine all central groupoids and to remove isomorphs.

The use of combinatorial values in the orderly algorithm proved to be very important, reducing the search time from over 360 minutes to less that 40.

It would be interesting to extend the results to an exhaustive list of central groupoids of order 16. To use the technique in [CDLP03], in their words, "seems prohibitively difficult."

The algorithms will need to be made more efficient in (probably) several ways in order to make that search. It might be feasible to define more combinatorial quantities on the graphs in order to lower the number of calls to `nauty`. The technique that GRAPE uses to call `nauty`, via text files and remote invocation of the program, is possibly also not very efficient, as the filesystem acts as a brake with every call. The process of obtaining all possible extensions to a partial rectangular structure and then reducing modulo the automorphism group is possibly acceleratable using some more efficient algorithm, perhaps even an orderly algorithm. Other analyses of the bottlenecks in this algorithm should be made.

This paper needs to be abbreviated, as a significant amount will be published in Theoretical Computer Science in 2004. I hope to make a new version of this paper explaining algorithmic improvements, but removing many other details covered in the other paper, when the algorithms get better.

The implementations in GAP4, as well as the resulting collections of examples, are available from the author electronically.

References

[CDLP03] Frank Curtis, John Drew, Chi-Kwong Li, and Dan Pragel. Central groupoids, central digraphs and zero–one matrices A satisfying $A^2 = J$. Unpublished manuscript, August 2003.

[Eva67] Trevor Evans. Products of points – some simple algebras and their identities. *Am. Math. Monthly*, pages 362–372, April 1967.

[FAYF85] M.A. Fiol, I. Alegra, J.L.A. Yebra, and J. Fàbrega. Digraphs with walks of equal lengths between vertices. In Y. Alavi, G. Chartrand, L. Lesnick, D.R. Lick, and C.E. Wall, editors, *Graph Theory with Applications to Algorithms and Computer Science*, pages 313–322. John Wiley, 1985.

[GAP02] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (`http://www.gap-system.org`).

[GR03] W. Guggenberger and J. Rung. L–Gruppoide: Algebraische und topologische Eigenschaften spezielle Gruppoide. *Contributions to Algebra and Geometry*, 44(1):263–283, 2003.

[Hof67] A.J. Hoffman. Research problem 2-11. *J. Combinatorial Theory*, 2:393, 1967.

[Knu70] Donald E. Knuth. Notes on central groupoids. *Journal of Combinatorial Theory*, 8:376–390, 1970.

[Lam75] C.W.H. Lam. On rational circulants satisfying $A^m = dI + \lambda J$. *Lin. Alg. App.*, 12:139–150, 1975.

[Lam77] C.W.H. Lam. On some solutions of $A^m = dI + \lambda J$. *J. Comb. Theory Ser. A*, 29:140–147, 1977.

[LvL78] C.W.H. Lam and J.H. van Lint. Directed graphs with unique paths of fixed lengths. *Journal of Comb. Theory B*, 24:331–337, 1978. In file.

[Ma84] S.L. Ma. On rational circulants satisfying $A^m = dI + \lambda J$. *Lin. Alg. App.*, 62:155–161, 1984.

[McK90] B.D. McKay. `nauty` user's guide. Technical report, Department of Computer Science, Australian National University, 1990.

[McK98] B.D. McKay. Isomorph-free exhaustive generation. *J. on Algorithms*, 26:306–324, 1998.

[McL54] David McLean. Idempotent semigroups. *American Math Monthly*, 64:110–113, February 1954.

[Men70] N.S. Mendelsohn. Directed graphs with the unique path property. In P. Erdos, A. Renyi, and Vera T. Sos, editors, *Combinatorial Theory and its Applications*, volume 4, pages 783–799. Colloquia Mathematica Societatis Janos Bolyai, 1970.

[Rea78] R.C. Read. Every one a winner. *Annals of Discrete Mathematics*, 2:107–120, 1978.

[Roy98] Gordon F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Mathematics*, 185:105–115, 1998.

[Rys70] H.J. Ryser. A generalisation of the matrix equation $A^2 = J$. *Lin. Alg. App.*, 3:451–460, 1970.

[Sha74] Leslie E. Shader. On the existence of finite central groupoids of all possible ranks. *J. Combinat. Theory Ser A*, 16:221–229, 1974.

[Soi93] L.H. Soicher. GRAPE: a system for computing with graphs and groups. In L. Finklestein and W.M. Kantor, editors, *Groups and Computation*, volume 11 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 287–291. A.M.S., 1993.

[Wan80] K. Wang. On the matrix equation $A^m = \lambda J$. *J. Comb. Theory Ser. A*, 29:134–141, 1980.

[Wan82] K. Wang. On the g–circulant solutions to the matrix equation $A^m = \lambda J$. *J. Comb. Theory Ser. A*, 33:287–296, 1982.

[YWH99] Qiao Li Yaokun Wu and Xuyan Huang. On the matrix equation $A^k = J - I$. *Linear Algebra and its Applications*, 295:249–260, 1999. in file.